CLAIMS

What is claimed is:

1. A method of verifying client authorization when requesting content and/or services from an application server, comprising the steps of:

generating a service ticket including a first copy of authorization data; and

sending a second copy of the authorization data to a client; and

sending the service ticket to the client.

2. The method as claimed in claim 1, further comprising the step of:

generating an AS_REP, including the service ticket and the second copy of the authorization data; and

sending the AS_REP to the client.

3. The method as claimed in claim 1, further comprising the steps of:

generating a ticket granting server reply (TGS_REP) including the service ticket; and

sending the ticket granting server reply to the client.

4. The method as claimed in claim 3, further comprising the steps of:

receiving an authentication server request (AS_REQ) message from a client;

generating an authentication server reply (AS_REP) message;

sending the AS_REP to the client;

receiving a ticket granting server request (TGS_REQ) message from the client; and

the step of generating the TGS_REP including generating the TGS_REP having two or more copies of authorization data including the second copy of the authorization data.

5. The method as claimed in claim 3, further comprising the steps of:

generating an authentication server reply (AS_REP) message including the second copy of the authorization data; and

sending the AS_REP to the client including the step of sending the second copy of the authorization data to the client.

6. The method as claimed in claim 3, further comprising the steps of:

configuring the second copy of the authorization data such that the second copy of the authorization data is used by the client.

7. The method as claimed in claim 6, further comprising the step of:

encrypting the second copy of the authorization data using a client session key.

8. The method as claimed in claim 7, further comprising the step of:

encrypting the service ticket using the server service key.

9. The method as claimed in claim 7, wherein the step of encrypting using the client session key including using the session key from a ticket granting ticket in an AS_REP.

10. The method as claimed in claim 6, further comprising the steps of:

the client determining desired content;

the client verifying the desired content with the second copy of the authorization data;

the client generating a request for content;

the client sending the request for content to a third party server; and

the third party server sending third party information to the client later used by the application server in determining client authorization for the requested content.

11. The method as claimed in claim 6, further comprising the steps of:

receiving a key request (KEY_REQ) from the client;

generating a key reply (KEY_REP);

forwarding the KEY_REP to the client;

the client generating a request for content;

the client verifying the request for content with the second copy of the authorization data; and

the client sending the request for content to an application server if the client verifies there are no errors in the request for content.

12. The method as claimed in claim 6, further comprising the steps of:

receiving a request for content;

sending at least a portion of the requested content to the client; and

the step of configuring the second copy of the authorization data including configuring the second copy of the authorization data such that the client is capable of

using the second copy of the authorization to determine at least an authorized use of the requested content.

13. The method as claimed in claim 12, further comprising the steps of:

the step of configuring the second copy of the authorization data such that the client is capable of using the second copy of the authorization to determine if the client is authorized to store the requested content.

14. The method as claimed in claim 13, further comprising the steps of:

the step of configuring the second copy of the authorization data such that the client is capable of using the second copy of the authorization to determine if the client is authorized to play back the requested content.

15. A system for providing secure communication across the system, comprising:

a key distribution center (KDC) first stage being configured to issue a ticket granting ticket (TGT) to a client; and

a KDC second stage being configured to generate a ticket granting server reply including at least two copies of authorization data in response to a TGT received from the client.

16. The system as claimed in claim 15, further comprising:

the client being configured to receive the ticket granting server reply and to utilize one copy of the authorization data to verify authorization.

17. The system as claimed in claim 15, further comprising:

the client being coupled with an application server, wherein the application server being configured to supply content to the client; and

the client being further configured to use the one copy of the authorization data to verify authorized use of the content.

18. A system for providing a client with access to content and/or services, comprising the steps of:

a means for generating a service ticket including a first copy of authorization data;

a means for generating a ticket granting server reply including the service ticket and a second copy of the authorization data; and

a means for sending the ticket granting server reply to a client.

19. The system as claimed in claim 18, wherein the means for generating the ticket granting server reply includes a means for encrypting at least the second copy of the authorization data using a client session key.

20. The system as claimed in claim 19, wherein the means for encrypting at least the second authorization data includes a means for encrypting at least the second copy of the authorization data such that the client is capable of decrypting and utilizing the second copy of the authorization data.

21. The system as claimed in claim 20, wherein the means for generating the service ticket includes a means for encrypting at least the first copy of the authorization data using a server key.

22. The system as claimed in claim 18, wherein the second copy of the authorization data being configured to allow the client to verify a request for services from an application server.

23. The system as claimed in claim 18, wherein the second copy of the authorization data being configured to allow the client to determine authorized use of received content.

24. A system for providing secure communication across the system, comprising:

a key distribution center (KDC) first stage being configured to issue a ticket granting ticket (TGT) and at least a client copy of authorization data to a client, wherein the client copy of the authorization data is configured such that the client is capable of determining client authorization; and

a KDC second stage being configured to generate a ticket granting server reply.